View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Embry-Riddle Aeronautical University

Publications

4-2013

Hazard Mitigation through a Systemic Model of Accident to a Socio-Technical System: A Case Study

Karim Hardy
Embry-Riddle Aeronautical University, hardyk1@erau.edu

Franck Guarnieri
Mines ParisTech

Follow this and additional works at: https://commons.erau.edu/publication

 Part of the Risk Analysis Commons

Scholarly Commons Citation

Hardy, K., & Guarnieri, F. (2013). Hazard Mitigation through a Systemic Model of Accident to a Socio-Technical System: A Case Study. *Journal of Energy and Power Engineering, 7*(4). Retrieved from https://commons.erau.edu/publication/497

This Article is brought to you for free and open access by Scholarly Commons. It has been accepted for inclusion in Publications by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

HAL
archives-ouvertes.fr

Hazard Mitigation through a Systemic Model of Accident to a Socio-Technical System: A Case Study

Karim Hardy, Franck Guarnieri

▶ To cite this version:

Karim Hardy, Franck Guarnieri. Hazard Mitigation through a Systemic Model of Accident to a Socio-Technical System: A Case Study. Journal of Energy and Power Engineering, 2013, 7 (4), p. 775-787 - Serial Number 65. <hal-00823248>

HAL Id: hal-00823248
https://hal-mines-paristech.archives-ouvertes.fr/hal-00823248

Submitted on 16 May 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

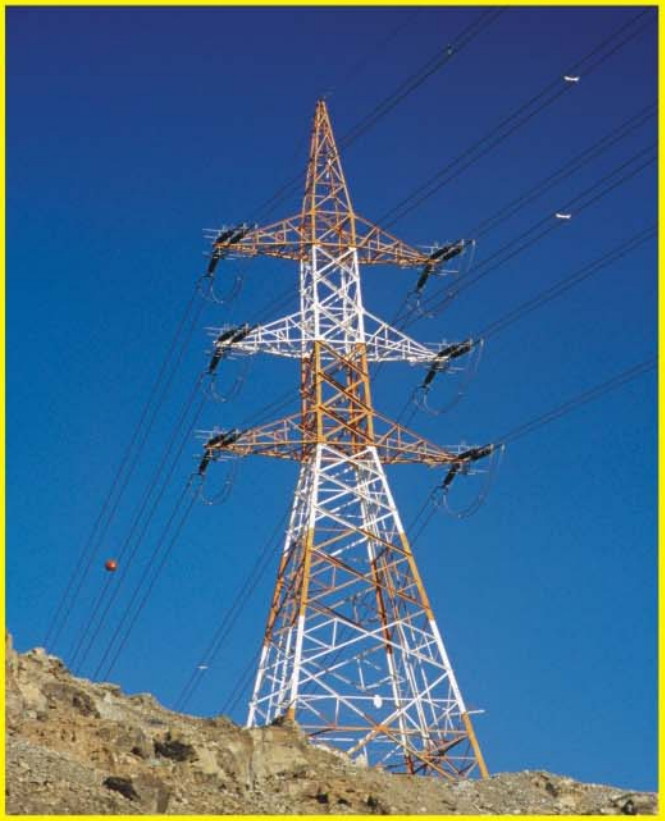
From Knowledge to Wisdom

JEPE

ISSN 1934-8975 (Print)
ISSN 1934-8983 (Online)

Journal of Energy and Power Engineering

Volume 7, Number 4, April 2013



David Publishing Company
www.davidpublishing.com

Journal of Energy and Power Engineering

Volume 7, Number 4, April 2013 (Serial Number 65)

David Publishing Company
www.davidpublishing.com

Journal of Energy and Power Engineering 7 (2013) 775-787

Hazard Mitigation through a Systemic Model of Accident to a Socio-Technical System: A Case Study

Karim Hardy[1] and Franck Guarnieri[2]

1. Aeronautics Department, Worldwide Campus, Embry-Riddle Aeronautical University, Daytona Beach FL 32114, USA

2. Center for Research on Risk and Crisis, Mines ParisTech, Sophia-Antipolis 06904, France

Received: April 26, 2012 / Accepted: August 08, 2012 / Published: April 30, 2013.

Abstract: This paper presents the STAMP (system-theoretic accident modeling and processes) accident model, based on systems theory, and describes its application in the context of risk prevention related to the remediation of contaminated sediments. The implementation of the model is described, and results are presented both in methodological and technical terms. The goal of this article is to emphasize the need of new approaches to take into account hazards and accidents within socio-technical systems.

Key words: Hazard analysis, hazards engineering, accident analysis, contaminated sediments, STAMP, systems theory, models.

1. Introduction

Remediation methods for contaminated sediments are now proved very effective in the treatment and management of contaminants. These methods use diverse techniques, and provide appropriate solutions for the treatment of sediment which originates from a variety of sources and has various consequences for the environment and people. However, these particularly novel and complex treatment technologies require a comprehensive hazard analysis. The analysis should aim to characterize all threats and risks (damage to people, equipment, local residents, the environment etc.), going beyond simple technical aspects related to the industrial process. This goal led to the search for a systems-based accident model, capable of meeting these criteria. The STAMP (systems-theoretic accident modeling and processes) accident model was chosen to characterize the dangers of an innovative remediation process known as Novosol®. The analysis was carried out through the application of the STPA (STamP-based analysis) technique, associated with the STAMP model.

The following text is divided into three parts. The first describes the problem of contaminated sediments and their danger to ecosystems and human health. Given these dangers, conventional treatment approaches are discussed. This first part also describes the Novosol® technology, a treatment process for contaminated sediments. The second part deals with the STAMP accident model developed at the MIT (Massachusetts Institute of Technology) by Professor Nancy Leveson, and the associated STPA technique, used for safety assessment. The third part presents the application of the STPA technique to the Novosol® system and outlines the results obtained. The aim here is to formulate safety recommendations focused on the overall socio-technical system in question.

2. Contaminated Sediments and Novosol®

This section discusses the issue of contaminated sediments. It is divided into three subsections. The first describes the environmental and health hazards arising from contaminated sediments. The second briefly discusses the treatment options available. The third

Corresponding author: Karim Hardy, research scholar, research fields: safety engineering, reliability, risk management within organizations. E-mail: hardykarim@gmail.com.

describes the Novosol® process (designed and developed by Solvay Company), of industrial treatment and remediation.

2.1 Contaminated Sediments: The Hazards

The natural environment is subject to numerous sources of contamination. Whether of industrial, urban or agricultural origin, they contain a rich variety of sedimentary pollutants. The damage caused by contaminated sediments has real environmental, social and economic costs. Not only are they the source of substantial loss of income due to the decline and contamination of animal and plant species, but they are also the cause of health problems for ecosystems and local populations. Dredging may also be required because sediments can cause an increased risk of flooding in certain areas, or reduce the draft of some waterways.

The main contaminants (cadmium, copper, chromium, lead, zinc, PCBs (polychlorinated biphenyls), PAHs (polycyclic aromatic hydrocarbons), and arsenic) arise from industrial activity (Table 1). The contamination they cause varies widely from one sediment to another and the health effects on both plant and animal populations can be dramatic (changes in, or destruction of aquatic ecosystems, development of pathological genes, etc.).

2.2 Contaminated Sediments: Treatment Solutions

The treatment of contaminated sediments poses significant technological, economic and environmental challenges. It can reduce pollution levels to the point

Table 1 Sources of sedimentary contaminants (the sign "●" means "a source of").

Industrial sector	Cadmium	Copper	Chrome	Lead	Zinc	PCB
Steel/iron				●	●	●
Aluminium	●		●			
Anti-fouling paint		●		●		
Electrical appliances	●	●		●	●	●
Automobile	●	●	●		●	●
Batteries				●		
Rubber					●	
Shipyards	●	●	●		●	●
Chemical	●		●			
Leather/tanning			●			
Detergents/surfactants					●	
Water/gas/electricity distribution					●	
Explosives		●				
Extraction of precious minerals				●	●	
Oxide production		●	●		●	
Metal finishing	●	●	●	●	●	
Steam power	●	●	●	●		
Electroplating		●	●	●	●	
Munitions		●			●	
Photography			●			
Pigments/inks				●		
Printing plates					●	
Plastics				●		
Metallurgical processes					●	
Oil refining				●		
Diverse sources	●	●	●	●	●	
Wastewater treatment		●	●	●	●	●

where sediments cleaned in this way can potentially be reused or recycled. The sediment is analyzed in order to select the appropriate technology and more importantly, to estimate the cost (Table 2). The fact that some processing techniques can themselves have an environmental impact, due to the release of contaminated water and/or gas into the natural environment needs to be taken into account. It must also be noted that all technical treatments of contaminated sediments that remove, store or treat contaminated sediment involve the breakdown and release of contaminants during the extraction operation.

Underwater sediments that are broken down in situ can cause contaminants to become suspended in the water column. The treatment solution must ensure that the level of these contaminants is as low as possible.

2.3 Treatment Solutions: The Novosol® Procedure

In 1993, Solvay SA began the development of Novosol® [1] initially to deal with fly ash from incineration then, from 1999, for a range of contaminated sediments. It responds to a wider need for the treatment of contaminated sediments and is operated under license by a company (or local collective) involved in environmental protection [2]. The process is divided into two treatment stages [3]:

Stage A: phosphation, which stabilizes heavy metals in the sediment (Fig. 1);

Stage B: calcination, which destroys organic matter and provides usable products such as bricks or material for making roads (Fig. 2).

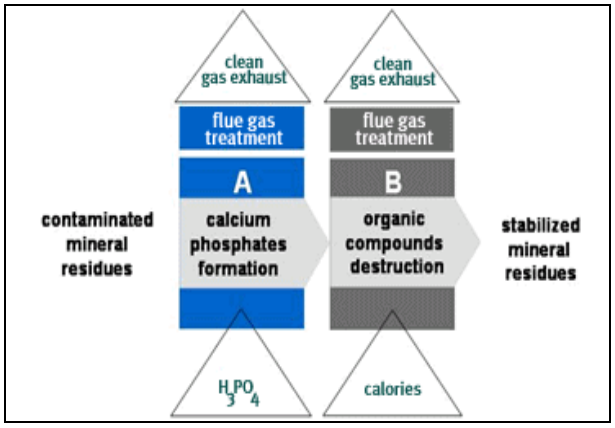


Fig. 1 Steps A and B of the Novosol® process. The two steps are complementary and independent, and produce no waste or liquid effluents. Stage A: heavy metals are stabilized by capturing them in a calcium phosphate matrix, Stage B: organic compounds are destroyed by calcination (650-900 °C = 1,200-1,650 °F) [3].

Table 2 Treatment techniques for contaminated sediments.

Treatment techniques	Application	Characteristics	Effectiveness	Cost
Biological treatments				
	Pesticides, hydrocarbons, PCBs, aromatic chlorides	pH 4.5-8.5 Temperature 59-167 °C Hydration 40%-80%	Depends on the volume to be treated	Fairly high
Physicochemical treatments				
Dechlorination	Dioxins, PCBs, chlorobenzene	pH > 2 Temperature 158-302 °C Hydration < 20%	> 98% effective for PCBs	High
Solvent extraction	PCBs, volatile organic compounds, aromatics, metals	Organic compounds < 40% Solid portion < 20%	Around 90% effective for PCBs	High
Soil leaching	Heavy metals, aromatics, PCBs, pesticides	Particle size 0.063-2 mm	90%-99% for volatiles and 40%-90% for semi-volatiles	High
Solidification/stabilization	Inorganic compounds, oily sludge and solvents		Fully effective on inorganic compounds	Relatively low
Thermal treatments				
Calcination	Volatile and semi-volatile compounds, dioxins	Hydration < 50% Particle size 1-2 mm	More than 99% for organic compounds	Very high
Desorption at low temperature	Volatile and semi-volatile compounds		99%	High

Fig. 2 An example of product re-use in road building [3].

A system like this, which brings together technology for the treatment of contaminated sediments and a large number of people on the ground, creates a high level of activity and risk, which must be controlled. Control is achieved through the application of the STPA risk analysis technique, which is associated with the systems-based accident model STAMP. STAMP facilitates a global risk analysis of the socio-technical system [4].

3. The STAMP Model and the STPA Technique

The accident model described in this section is a systems-based model. It was developed in the 2000s by Professor Nancy Leveson at the Complex System Research Laboratory of the MIT (Massachusetts Institute of Technology), and addresses the limitations of traditional accident models. This section is divided into three subsections. The first highlights the value of systems-based accident models in general. The second describes the STAMP model in particular. The third describes the STPA technique which has been developed from the STAMP model.

3.1 Systems-Based Accident Models

Any complex system has its own dynamics which have evolved during its lifetime, and are the results of the activities that link its elements. This dynamic is subject to the interplay of various factors, which follow certain rules and principles and which, over time, control the system state. Seen from a system safety perspective, the challenge is to always keep in mind that in such a dynamic system, a stable dynamic system state can become an unstable dynamic state. Modern technologies have a significant impact on the very nature of accidents and risks. In order to understand them, new explanatory mechanisms must be established. At the same time new techniques for risk assessment must be developed to prevent accidents occurring [4].

Systems-based accident models enable a better description and understanding of the links between diverse factors across different hierarchical levels. They thus facilitate the study of problems in a way which makes it possible to have a global view of the socio-technical system. Systems-based accident models are distinguished from other models in that they describe the process of an accident as a set of interconnected and complex events, while sequential models [5] and organizational models [6] simply present a linear description of the accident. In systems-based models, an accident occurs when several factors (human, technical, environmental) come together in a specific place and time [7].

Models based on systems theory view accidents as emergent phenomena which are the result of interactions between components of a system. Interactions between these components are nonlinear and consist of many feedback loops [8]. In effect, safety is only established by interactions between elements of a system and does not constitute the property of an individual element. Systems models derive from general systems theory [9] which proposes principles, models and laws in order to understand relationships between the elements of a complex system. From this perspective, a system is not seen as a static representation, but rather as a dynamic process, constantly adapting in order to achieve its objectives and responding to internal and external changes.

Systems-based accident models therefore aim to study the dynamic, nonlinear properties of the system and the migration of an organization under stress into a dangerous or even accidental state. The proactive nature of these accident models (in terms of risk prevention) means that they can address problems that affect the system as a whole, rather than focusing on specific problems associated with isolated errors, taken out of context. This type of model can also take into account dynamic aspects by modeling this migration within organizations that are subject to various global and environmental pressures related to their activities and/or issues.

3.2 The STAMP Model

The STAMP accident model is based on systems and control theory [4]. It was developed by Professor Nancy Leveson (MIT). In the STAMP model, safety is viewed as a control problem. The STAMP model is constructed from three interrelated concepts (safety constraints, hierarchical control structures and process models), described below:

- Safety constraints: The concept of constraint is at the heart of the STAMP model. In systems theory, control always calls for the integration of constraints. An accident is not seen as the result of a series of events, but as a deficiency or lack of integration of constraints at each level of the socio-technical system. Safety constraints target the relationships and decisions between the many and various system variables. These constraints are also associated with a control process which aims to manage changes and adaptations in system behavior. Unlike the classical vision of the accident (that it is due to a sequence of events) in STAMP terms, accidents are viewed as the inadequate enforcement of constraints within a socio-technical system;
- Hierarchical safety control structures: Accident prevention or analysis requires the design of a control structure that includes a description of the socio-technical system which is as representative as possible of a given context. This structure takes into account constraints required during both the development of the system, and its subsequent operation in accordance with functional requirements. A control structure can be developed for each subsystem of a larger system. Systems theory understands a system as a hierarchical structure in which each level imposes constraints on the activity of the level below it [4, 10]. Accidents result from the inadequate enforcement of constraints within the hierarchical levels of a given socio-technical system;
- Process models and control loops: A control process (within a process model) operates between each level of the hierarchy described above. The purpose of the control process is to translate an "input" from one hierarchical level into a "control" over another hierarchical level. This control process can operate both upwards and downwards though the hierarchy. It is represented diagrammatically as a control loop which describes the control process. In complex systems, one or more control loops link the hierarchical levels of each control structure, with a downlink channel providing the information and controls necessary to impose constraints on the lower level, and an uplink channel which feeds back the effectiveness of these constraints. At each level of the control structure, inadequate control may result from neglect of safety constraints, poor communication of safety constraints or safety constraints incorrectly applied at the lower level. This is why feedback represents such an important dimension in the operation of a system. For example, the constraints generated by the safety analysis process always include assumptions about the operating environment of the process. When the environment changes, these assumptions become false, and the controls in place are no longer appropriate. This discrepancy between the environment and the system can become the cause of a de-synchronization and the source of inappropriate or even dangerous behavior.

The effective implementation and operation of the STAMP model is achieved through a technology known as STPA, presented in the next section.

3.3 The STPA Technique

STPA is a systems safety technique developed from the STAMP accident model [11]. STPA hazard analysis (STamP-based Analysis) was described by Leveson and her team [4-12]. The analysis has two main objectives: accident investigation and safety assessment. STPA hazard analysis is an iterative process which facilitates analysis of the origins and causes of an accident. In STPA analysis, the system is seen as a set of control loops which interact with each other. An accident is therefore the result of an inadequate control.

STPA analysis can be used for both accident prevention and to evaluate the safety level of a system. In the latter case, the aim is to collect information that drives a safety-oriented approach to design and development. Hazard analysis is essentially a procedure which aims to prevent accidents before they happen. A proactive approach to accident prevention, based on the STAMP model, may provide the information necessary for risk prevention and thus the occurrence of accidents.

Current hazard analysis techniques, such as those found in operational safety, are not equipped to take into consideration the dynamic and complex nature of modern systems, in which human-machine interactions are important. That said, the objectives of an STPA hazard analysis are broadly similar to those of a traditional hazards analysis.

On the one hand, it aims to identify hazards throughout the life-cycle of a system as well as safety constraints associated with the maintenance of an acceptable level of safety;

On the other hand, it aims to determine how safety constraints may be violated and how such constraints can lead to inappropriate actions which push the system toward an accidental state.

The STPA hazard analysis process is divided into five stages (Fig. 3):

Stage 1: consists of a preliminary analysis of system risk, and in the definition of requirements and constraints applicable at the level of the system, in order to define safety requirements and constraints to be applied to the system as a whole.

Stage 2: consists of the establishment of the safety control structure (the roles and responsibilities of the elements and feedback mechanisms). It allows the establishment of the safety control structure for the system, which include the roles and responsibilities of each element, both control elements and feedback. This stage will ultimately define and establish the control structure for system safety as described by Leveson [10]. Every level or element of the control structure has roles and responsibilities that help determine whether system safety constraints are applied or not. Once the system elements to be included have been defined, the safety control structure must be modeled.

Stage 3: aims to integrate system requirements and constraints for each element of the system. The system requirements and constraints defined in Stage 1 must be integrated for each element of the safety control structure defined in Stage 2.

Stage 4: involves a detailed analysis of the control structure and process models in order to identify inadequate controls actions which may play a role in the occurrence of an accident. In order to do this, inadequate controls actions are classified into four types [1]:

- A control action was not executed;
- An inappropriate or ineffective control action was executed leading to a failure;
- A potentially correct control action took place too early, too late, or at the wrong time;
- A correct control action was stopped too early.

Stage 5: is a temporal (immediate, long-term, standard) categorization of identified risks (defects in control loops). This categorization is done primarily to

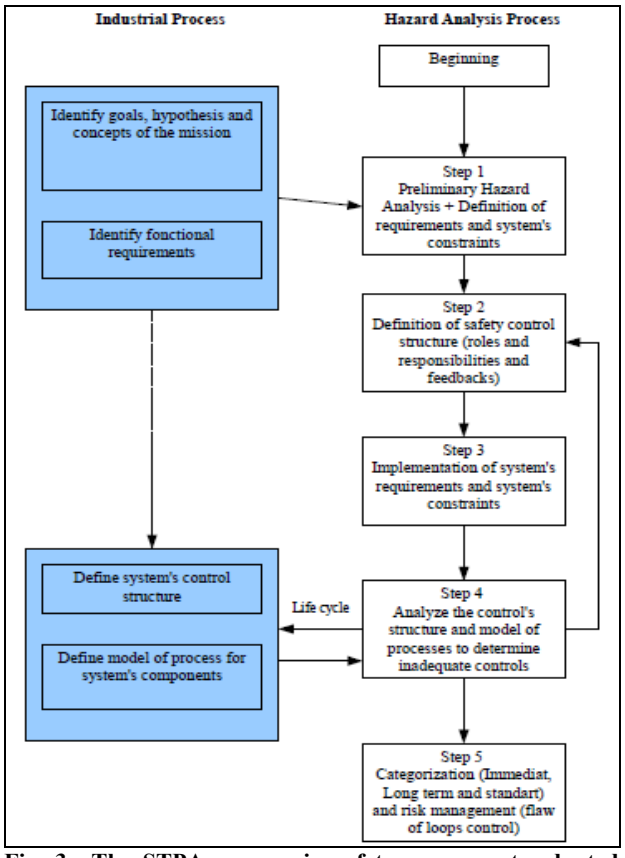


Fig. 3 The STPA process in safety assessment, adapted from Leveson et al. (2004).

determine the impact of inadequate control actions on system behavior. Control defects are then dealt with by identifying the processes that could lead to a breach of one or more safety constraints.

These five stages together form the STPA methodology which is the backdrop for the implementation of the STAMP model in an industrial setting. The remediation of contaminated sediment (carried out using a physicochemical process called Novosol®) was selected as the field of analysis to make the demonstration. The whole application is described in the next section.

4. Applying the STPA Technique to the Novosol® Program

In this section, each stage of the STPA methodology presented above is revisited and described in the context of Novosol® as a socio-technical system [1]. The level of complexity is directly affected by the numerous participants involved in the procedure. Implementation of the Novosol® program requires the development of a Nosovol® facility. In this example, the facility is managed by Company A, who are in direct contact with Company B. Company B is in charge of the operation of the Novosol® process.

This section is organized into five subsections which illustrate each of the five stages of the application of the STPA technique to the Novosol® program.

4.1 Stage 1: Preliminary Risk Analysis and Definition of Requirements and Constraints at System Level

During a safety assessment, a preliminary risk and hazards analysis is performed at system level, in order to define the safety requirements and constraints to be integrated. It must be carried out in the early stages of the life-cycle of the socio-technical system. This preliminary system risk analysis, when applied to the Novosol® system, consists of two levels of analysis. The first concerns the technical implementation of the Novosol® process, while the second focuses on the socio-technical aspect of the system, and includes all actors in the system and their interactions. This approach meets the requirements of the Solvay SA group, and the methodology of the STPA hazard analysis technique.

An initial investigation was undertaken in response to a request from industry for a risk management analysis of the Novosol® system. The request concerns risk assessment of the phosphation phase of the technical process.

An occupational risk assessment was carried out using compliance and risk analysis software (http://www.preventeo.com) followed by a HAZOP[1] analysis. It was apparent that the HAZOP methodology is suited to the analysis of the physicochemical aspects of the Novosol® procedure

[1] HAZOP [3] is a technique for hazard analysis which aims to identify deviations in a system or process, often physical and/or chemical.

[11], and also underlined the fact that, like the STPA technique, HAZOP methodology looks for potential differences between the desired state of the system and its actual condition. However, while HAZOP focuses on technical parameters in a technical system, STPA deals with control problems in a socio-technical system, taking into account human and organizational factors. The HAZOP-based analysis was used to characterize the initial safety constraints of the phosphation phase of the Novosol procedure, which are focused on process engineering.

This set of analyses[2] led to the formulation of safety recommendations to improve both the design of a future Novosol® installation and safety levels in preparation for becoming fully operational. They were supplemented by a second study and subject to a more comprehensive analysis. This second study focused on Novosol® as a socio-technical system. It included both human and organizational factors at the site, as well as the companies involved in the evolution of Novosol®, in terms of its development and operation.

System requirements and constraints are defined for each hierarchical level of the system. In this way, for the company operating the Novosol® process (Solvay SA during the technological development phase) and in the current context, requirements and constraints can be identified, using the STPA method. They are shown in Table 3.

Taken together, the definitions of requirements and constraints for each of the hierarchical levels enable the hierarchical control structure to be established.

4.2 Stage 2: Establishment of the Safety Control Structure

This second stage allows the construction of the safety control structure of the system in question, including the roles and responsibilities of each element (control elements and their feedback loops) [13, 14].

The definition and establishment of the system safety control structure [10] is the cornerstone of this STPA stage, each level or element of the control structure has roles and responsibilities that aimed at ensuring system safety constraints are applied within the system. Once the safety control structure has been defined, it is necessary to model it.

The model is built by linking the various hierarchical levels using the interactions between elements. This stage includes all the actors defined in Stage 1, when the requirements and constraints of the Novosol® system were established.

This stage not only provides an overview of the system in question, but also highlights the interactions between levels in the hierarchy. The control structure integrates roles and responsibilities. This makes it easier to determine the influence elements have on each other (Fig. 4). The structure provides a static overview of the whole Novosol® system, showing the roles and responsibilities at each hierarchical level. These roles and responsibilities are used to support the definition and integration of constraints (identified in Stage 3) at the level of each actor in the structure.

The purpose of the structure thus defined is to represent the interactions between different hierarchical levels, and to characterize the controls between elements. It sets limits for the analysis that will subsequently determine potentially inadequate controls between levels.

4.3 Stage 3: Integration of System Requirements and Constraints at the Level of the Element

The system requirements and constraints defined in Stage 1 must be integrated into each hierarchical level of the safety control structure defined in Stage 2. This third stage is based on the previous two, and aims to integrate safety requirements and constraints within each hierarchical level. This is done taking into account the various interactions between elements. This stage allows the definition of requirements which are translated into safety constraints, given the various interactions between elements of the safety control structure.

[2] Reports containing the results of this work were delivered to Solvay SA in 2009.

Table 3 Sample requirements and constraint definitions for the controller (the operating company).

Company operating Novosol® (Company B)
Safety constraints and requirements
Treatment of sediments contaminated by organic compounds and heavy metals
Responsible for the smooth conduct of inspections and preparation of reports on the use and development of Novosol® in collaboration with national and international bodies
Responsible for defining operational requirements and performance of Novosol® in accordance with national and international regulations

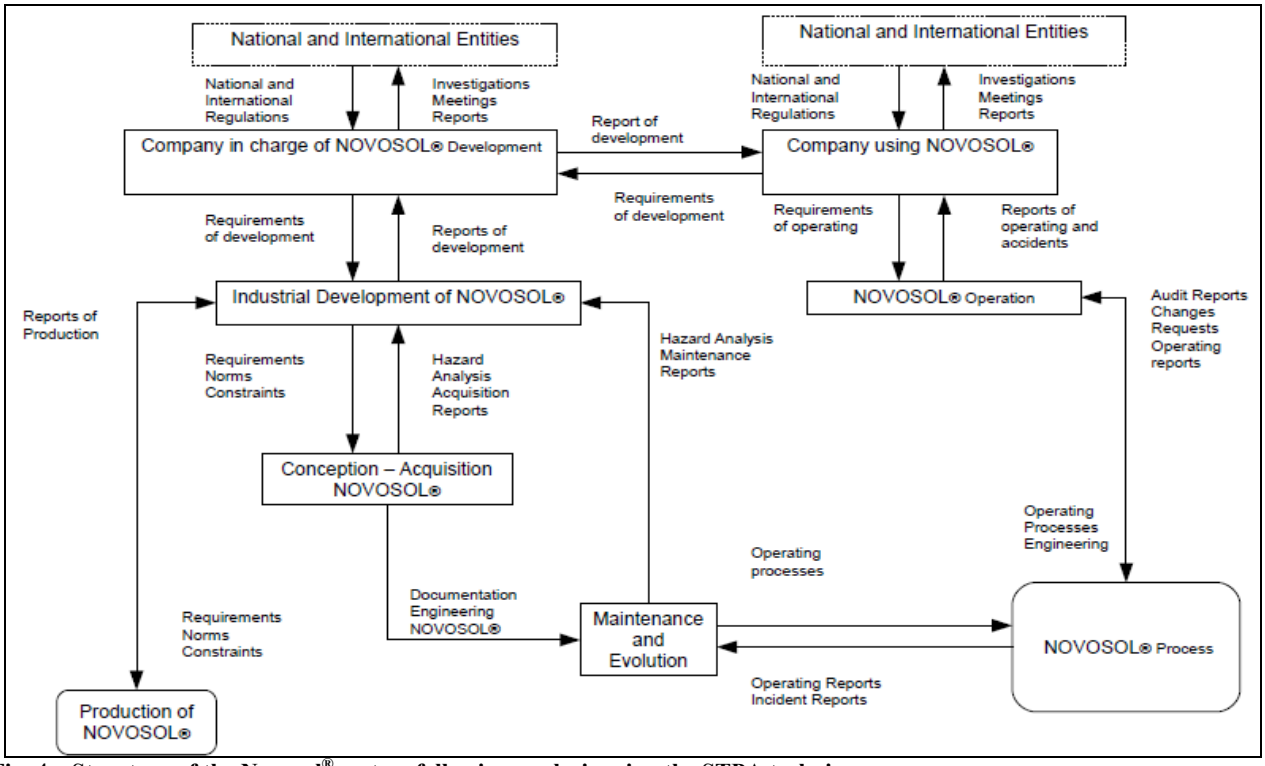


Fig. 4 Structure of the Novosol® system following analysis using the STPA technique.

From Fig. 4, the higher hierarchical level—for example the decision-making level of the company responsible for the development of Novosol® (Company A)—sets developmental requirements for the lower hierarchical level (the industrial development of Novosol®). This lower level must provide feedback (control checks) through the submission of development reports to the higher level (the decision-making level of Company A). This is the case for each interaction and each variable.

In practical terms (at this level of the structure), the decision-making level of Company A must define and provide requirements for the development of a Novosol® facility to the service or entity responsible for industrial development. In return, and in order that management of Company A is informed of the successful integration of these developmental requirements (controls), the service or entity provides development reports describing the progress of the project, including any potential difficulties.

Specifically, for the two hierarchical levels "the decision-making level of the company responsible for the development of Novosol®" and "the industrial development Novosol®", the wording might be: "The decision-making level of the company in charge of the development of Novosol® (Company A) must provide developmental requirements to the level responsible for the industrial development of Novosol® (Company A)". In return, "the level responsible for the industrial development of Novosol® (Company A) must provide

reports indicating the progress of development to the decision-making level of the company responsible for the overall development of Novosol® (Company A)".

4.4 Stage 4: Detailed Examination and Analysis of the Control Structure and Process Models for Inadequate Controls

In this stage, a detailed analysis of inadequate controls is required. The analysis helps to identify potentially inadequate controls which may lead to an accident. The analysis is based on identification of the four types of inadequate controls described in Stage 4 of the STPA methodology (see Section 3.3). This analysis leads to the definition of actual inadequate control measures (or potential in the case of a safety assessment). For each hierarchical level, inadequate controls are defined using the relationships established when the control structure was constructed (Table 4).

Collectively, inadequate control measures are translated into constraints and safety requirements which have to be integrated at the level of each system element (Table 5).

This translation of potential inadequate and defective controls forms an inventory of defects and dangers that could lead the system towards an accidental state. This list allows the definition of the constraints that each hierarchical level must respect in order to maintain an acceptable level of safety. These inadequate control actions and constraints are termed "potential" because they are assumed to exist and are only defined in the context of a safety assessment.

4.5 Stage 5: Categorization of Identified Risks

The first step is to categorize the risks identified in order to determine the impact of inadequate control actions on the behavior of the system. The second step is to implement a risk management strategy through the identification of the process(es) leading to the breach of one or more safety constraints. This step aims to create a hierarchy of control defects. It aims to optimize system safety by first, quickly addressing immediate risks that might migrate the system to an accidental state, then addressing long-term risks (which could lead to an accident at some point in the future), then finally tackling "standard" risks which are dealt with using a risk management strategy during the life-cycle of the system.

The challenge here is to identify which safety recommendations need to be implemented as a priority. The identification made it necessary to identify in a control loop, a safety constraint may be violated. At each level of the loop, and in each interaction between loop levels, there may be inadequate controls. The goal is, for each hierarchical level, to identify inadequate controls that can migrate the system to an accidental state. During execution of the loop each of these controls may result in the creation of an inadequate output control at another level, resulting in the migration of the system (Fig. 5) into an unstable state.

Fig. 6 illustrates the "maintenance" level. This description of the control loop is simplified, i.e., potentially inadequate controls within it are not included.

The "maintenance" control loop, highlighting the collection of elements involved in the control process at this level, in interaction with the levels "industrial development" and "design". Based on Fig. 5, this control

Table 4 Inadequate control actions for the controller (the company operating Novosol®).

Company operating Novosol® (Company A)
(Potential) inadequate control measures
The decision-making level of the operating company does not provide operating requirements for the safe use of Novosol® to the operational level
The decision-making level of the operating company does not make their developmental requirements known to the decision-making level of the company responsible for the development of Novosol® (Company A)
The decision-making level of the operating company does not provide inspection reports to control bodies

Table 5 Potential constraints on the controller (the company operating Novosol®).

Company operating Novosol® (Company A)
(Potential) constraints
The decision-making level of the operating company must provide operating requirements for the safe use of Novosol® to the operational level
The decision-making level of the operating company must make their developmental requirements known to the decision-making level of the company responsible for the development of Novosol® (Company A)
The decision-making level of the operating company must provide inspection reports to control bodies

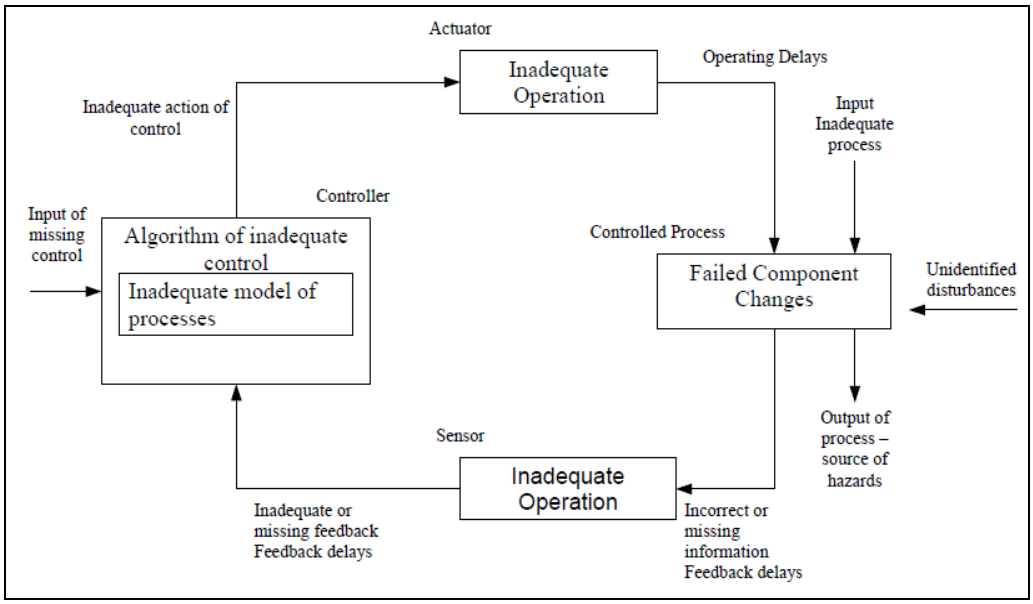


Fig. 5 Inadequate control loop. Actions carried out within the control loop may lead to an inadequate control. These potential actions must be identified so that the hierarchical level can provide adequate control.

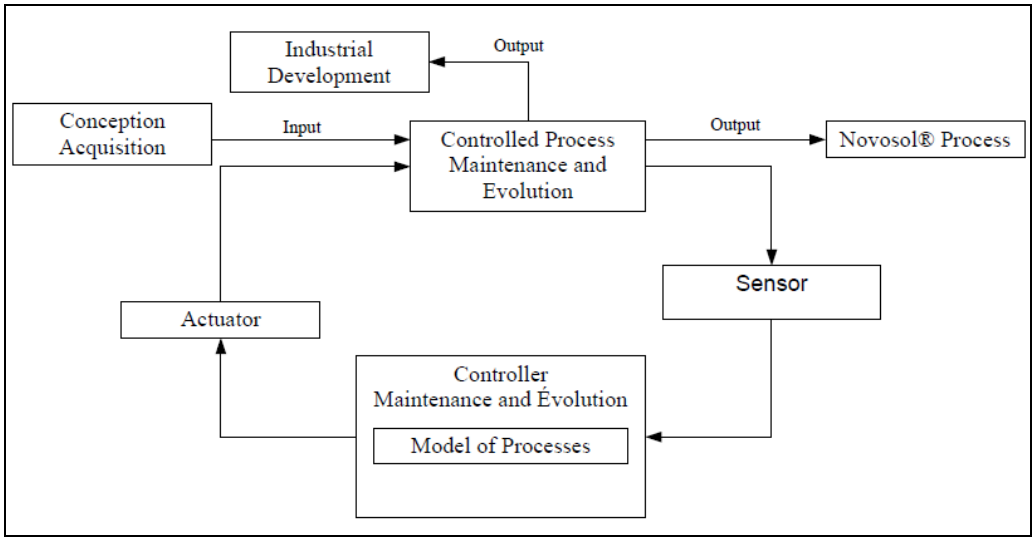


Fig. 6 The "maintenance" control loop [1].

loop may contain incorrect information that could cause an inadequate control output to the "design" and "industrial development" levels.

This and all other loops in the control structure are part of the Novosol® system and it is therefore essential to analyze them from the point of view of the entire system in order to determine the potential source of inappropriate controls (Fig. 7).

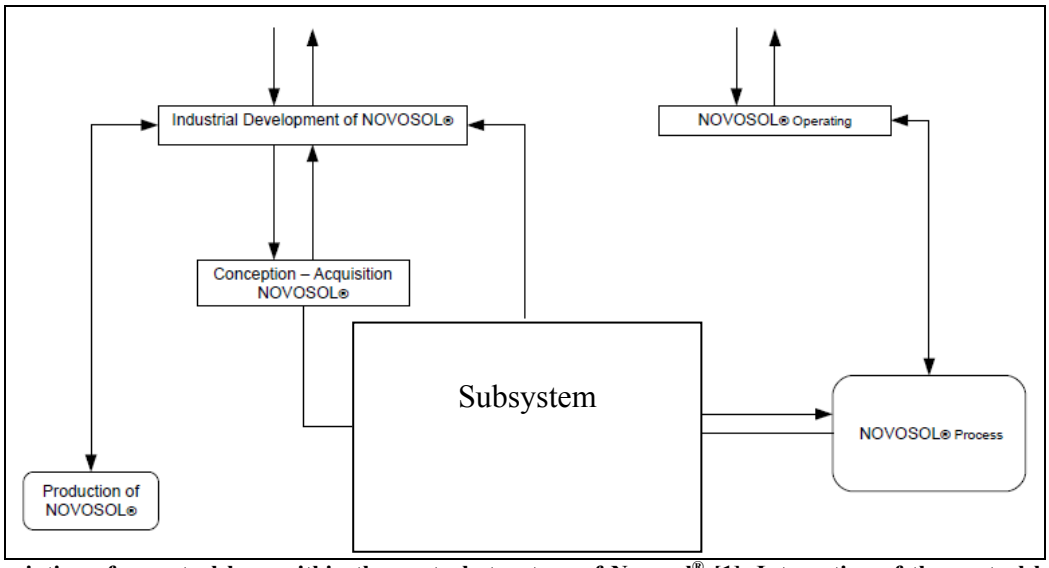


Fig. 7 Description of a control loop within the control structure of Novosol® [1]. Integration of the control loop into the control structure illustrates how a given hierarchical level interacts with the rest of the control structure.

This phase of risk categorization begins with the development of a Novosol® installation, in the analysis of existing control loops, and continues throughout its life-cycle, as the organization of the control loops changes.

5. Conclusion

This article has presented a systems-based accident model called STAMP (developed at MIT) and applied it to a system for the treatment of contaminated sediments.

The application of a systems-based accident model to the treatment of contaminated sediments contributes greatly to so-called traditional model of accidents. The study of system risk at an organizational level, rather than technical risks at a "field" level, can open roads to improved solutions for the treatment and recovery of contaminated sediments. A task in every day becomes a little more complex.

Acknowledgments

The authors would like to thank:

- Solvay SA and especially Guy Depelsenaire for funding this research. Solvay SA is a Belgian chemical company active in two major sectors: chemicals and plastics;
- ANRT (National Association of Technological Research), for providing a grant to carry out this work. ANRT is a French research and development non-profit organization (including both public and private sector businesses) which aims to optimize innovation and research in France;
- The MIT (Massachusetts Institute of Technology) and especially Nancy Leveson (Complex Systems Research Laboratory), for hosting me for six months in order to conduct research on the STAMP model. The Complex Systems Research Laboratory is headed by Professor Nancy Leveson who is responsible for developing the STAMP Model.

References

[1] K. Hardy, Contribution to the study of a systemic model of accident: The case of STAMP: Application and Improvements, Ph.D. Thesis, Centre de recherche sur les Risques et les Crises, Mines ParisTech, 2010.

[2] D. Breugelmans, Novosol®: The story of a pluridisciplinar step by step approach, environmental research and development, Solvay S.A. Web site, 2007, http://www.novosol.be/static/wma/pdf/1/0/5/5/9/Reusedfinal.pdf.

[3] Solvay SA. Novosol® Home Page, 2012, http://www.novosol.be.

[4] N.G. Leveson, A new approach to hazard analysis for

complex systems, in: International Conference of the System Safety Society, Denver, CO, 2003.

[5] J. Reason, Managing the Risks of Organizational Accidents, Ashgate Publishing, UK, 1997.

[6] K.H. Roberts, Managing high reliability organizations, California Management Review 32 (4) (1990) 101-113.

[7] E. Hollnagel, Barriers and Accident Prevention, Ashgate Publishing, Sweden, 2004.

[8] C. Perrow, Normal Accidents: Living with High-Risk Technologies, Princeton University Press, Princeton, NJ, 1999.

[9] L. Bertalanffy, General System Theory, George Braziller, New York, 1968.

[10] N.G. Leveson, A new accident model for engineering safety systems, Safety Science 42 (4) (2004) 237-270.

[11] C.A. Ericson II, Hazard Analysis Techniques for System Safety, Wiley-Blackwell, USA, 2005.

[12] N.G. Leveson, M. Daouk, N. Dulac, K. Marais, A systems theoretic approach to safety engineering: A case study, in: MIT Engineering Systems Division External Symposium. Cambridge, MA, 2004.

[13] K. Hardy, F. Guarnieri, Modelling and hazard analysis for contaminated sediments using the STAMP model, in: 14th International Conference on Process Integration, Modelling and Optimisation for Energy Saving and Pollution Reduction, Florence, Italy, May 8-11, 2011. (in press)

[14] N.G. Leveson, A New Approach to System Safety Engineering, Unpublished Manuscript, Cambridge, MA, 2006.

Journal of Energy and Power Engineering
Volume 7, Number 4, April 2013

David Publishing Company
9460 Telstar Ave Suite 5, EL Monte, CA 91731, USA
Tel: 1-323-984-7526, 323-410-1082; Fax: 1-323-984-7374, 323-908-0457
http://www.davidpublishing.com, www.davidpublishing.org
energy@davidpublishing.com, energy@davidpublishing.org, energy-power@hotmail.com

ISSN 1934-8975 04
9 771934 897134